

Zusammenfassung meines Vortrages vom 12. März 2018

# Überwachung unserer digitalen Lebensräume

Andreas Grimmer  
Pro Scientia, Gruppe Linz  
contact@andreasgrimmer.com

---

In dieser Zusammenfassung beleuchte ich, passend zu unserem diesjährigen Jahresthema, wie unsere *digitalen Lebensräume* überwacht werden. Dazu gehe ich in meiner Ausarbeitung auf das Sicherheitspaket mit Schwerpunkt “Bundestrojaner” näher ein, welches dieses Jahr der Bundesregierung vorgelegt wird.

## 1 Einführung

Das geplante Sicherheitspaket sieht eine Ausweitung der Überwachungsmöglichkeiten vor und umfasst im Wesentlichen den polizeilichen Zugriff auf den Großteil der Videoüberwachung im öffentlichen Raum, ein Verbot von anonymen Wertkartenhandys, eine abgeschwächte Vorratsdatenspeicherung und einen “Bundestrojaner”. Der aktuelle Stand (Zeitpunkt des Vortrages war der 12. März 2018) dieses Sicherheitspaketes ist wie folgt:

- Die Bundesregierung hat am 21. Februar 2018 ein Überwachungspaket vorgelegt.
- Am 21. Februar 2018 wurde das Sicherheitspaket im Ministerrat beschlossen.
- Im nächsten Schritt wird das Paket im Nationalrat eingebracht.
- Geplant ist, dass der Großteil der Maßnahmen mit 1. Juni 2018 in Kraft treten wird.

Da besonders der Bundestrojaner ein sowohl parteipolitisch als auch gesellschaftlich kontroversiell diskutierter Aspekt dieses Sicherheitspaketes ist, habe ich mich in meiner Präsentation und Zusammenfassung entschieden, auf diesen näher einzugehen.

## 2 Bundestrojaner

Der Bundestrojaner ist eine staatliche Spionagesoftware, die der Überwachung von verschlüsselter Kommunikation (z.B. von WhatsApp oder Skype Nachrichten) dienen sollte. Da der Inhalt von verschlüsselten Nachrichten nicht von möglichen Mithörern entschlüsselt werden kann (vermutlich auch nicht von Geheimdiensten), muss ein sogenannter *Trojaner* auf dem Gerät, welches die Nachrichten sendet/empfängt, installiert werden. Ein Trojaner ist ein Programm, das auf einem Computer, Smartphone oder einem anderen elektronischen Kommunikationssystem heimlich oder als nützliches Programm getarnt Funktionen ausführt, die der Benutzer nicht erlaubt hat und nicht kontrollieren kann. Ein Trojaner erlaubt die Installation von Schnüffel-Software (engl. *Spyware*) oder beinhaltet diese bereits. Die

Funktionalität der Spyware reicht von der Aufzeichnung der Eingaben (mittels Keyloggern) bis hin zur Datenanalyse und Weiterleitung der gesamten Kommunikation. Somit können die am Endgerät noch unverschlüsselten Nachrichten abgefangen und weiterverarbeitet werden.

Die gezielte Installation eines Trojaners auf dem Gerät, welches überwacht werden sollte, ist eine schwierige und aufwendige Operation, weil dazu die Hardware- und Software-Konfiguration des Zielsystems zuvor der Behörde bekannt sein muss. Nach der Ausspähung können folgende Techniken zur Installation des Trojaners zum Einsatz kommen:

- Phishing (ist der gezielte Versand von E-Mails oder SMS, deren Anhänge den Trojaner beinhalten)
- Verseuchte Websites und gefälschte Apps
- Manipulierte Anhänge einer E-Mail von Bekannten und manipulierte Downloads
- Physischer Zugriff und händische Installation
- “Herumliegenlassen” von CDs, USB-Sticks
- Verwendung von dafür vorgesehenen Hintertüren durch den Hersteller
- Verwendung von Sicherheitslücken in Software oder auch Hardware

Nach der Infiltration des Zielsystems können Kommunikation und Daten des Adressaten analysiert und auf einen Server übertragen werden. Die Auswertung dieser Daten erfolgt schließlich manuell von der Behörde.

Eine derartige Spionagesoftware sollte voraussichtlich im Jahr 2020 zum Einsatz kommen und wird etwa bei Verbrechen mit einer Strafobergrenze von mehr als zehn Jahren, bei einem Verdacht auf terroristische Straftaten, bei Straftaten gegen Leib und Leben oder bei Straftaten gegen die sexuelle Integrität mit einer Strafobergrenze von mehr als fünf Jahren gerechtfertigt. Das heißt, der Einsatz des Bundestrojaners ist nur für Einzelfälle geplant.

### 3 Konklusion

Durch einen Beschluss des geplanten Sicherheitspaketes werden die Rechte für eine Überwachung unserer digitalen Lebensräume sicherlich ausgeweitet. Neben der teils technisch schwierigen und teuren Umsetzung (besonders beim Bundestrojaner) erscheint es mir wichtig, dass *vor* der Einführung alle Inhalte dieses Sicherheitspaketes sehr kritisch hinsichtlich derer gesellschaftlicher Auswirkungen analysiert und evaluiert werden.

### Literatur

- [1] H. Pohl, “Zur Technik der heimlichen Online-Durchsuchung,” *Datenschutz und Datensicherheit-DuD*, vol. 31, no. 9, pp. 684–688, 2007.
- [2] M. Hansen, A. Pfitzmann, and A. Roßnagel, “Online-Durchsuchung,” *Deutsche Richterzeitung*, vol. 8, p. 225, 2007.